Challenges to Multi-Enterprise Integration
the EECOMS Experience

William J. Tolone[1], Bei-tseng Chu[1], Gail-Joon Ahn[1], Robert G. Wilhelm[1], and John E. Sims[2]
[1]*University of North Carolina at Charlotte, USA,* [2]*IBM Corporation, USA,*
wjtolone@uncc.edu

Abstract: The EECOMS Project is a multi-company and university joint effort to research and develop intelligent, dynamic technologies for integrating supply-chain planning, scheduling, and execution and for enabling the evolution of such multi-enterprise integration solutions. In this paper, we describe several critical challenges to enterprise integration in the form of "lessons learned" by the Project in its effort to develop leading edge multi-enterprise integration solutions. These lessons reflect the human side of enterprise integration, the integral role of security and privacy, and the re-examination/definition of traditional business processes that enterprise integration requires.

1 INTRODUCTION

Advances in Information Technology (IT) have transformed the conduct of business. As IT has matured, more and more business processes have been automated. Recent attention has focused on the integration of individual processes across the business enterprise (e.g. WebSphere, MQSI, Neon, RosettaNet, CommerceNet, OAGIS). Enterprise Integration (EI) refers to the methodologies and technologies that support these efforts. The purpose of this paper is to describe several critical challenges to EI as "lessons learned" by one large-scale effort, the EECOMS Project (NIST ATP 97-05-0020, 1998), to develop leading edge multi-enterprise integration solutions. We begin with a brief overview of the project. Next, we highlight three important lessons learned in regards to Enterprise Integration.

K. Kosanke et al. (eds.), *Enterprise Inter- and Intra-Organizational Integration*

- **Lesson One:** People are Essential Participants in Enterprise Integration
- **Lesson Two:** Security and Privacy are Integral to Enterprise Integration
- **Lesson Three:** Effective Enterprise Integration Often Requires a Re-examination/definition of Traditional Business Processes

We conclude with some reflections on the EECOMS experience, discussing some strengths and weaknesses of a consortium-based approach (involving both industry and academia) to research and develop leading edge enterprise integration solutions.

2 THE EECOMS PROJECT

In 1998, the EECOMS Project was established as the second project managed under the CIIMPLEX joint venture agreement (CIIMPLEX, http://). EECOMS stands for the *Extended-Enterprise Consortium for Integrated Collaborative Manufacturing Systems*. Support for the three-year project originated through a government/private-sector partnership program. Federal support totaling $14.5M came from the Department of Commerce's National Institute of Standards and Technology, Advanced Technology Program (NIST/ATP). The mission of the NIST/ATP program is to strengthen the U.S. economy through high-risk, leapfrog technologies that broaden both participant and national competencies with the potential for broad base diffusion. Private-sector support totaling $15M came from the project's industry partners: BAAN SCS, Boeing, Envisionit, IBM, INDX, Scandura, TRW, and Vitria Technologies.

Key to this government/private-sector partnership was the inclusion of three universities: the University of North Carolina at Charlotte, the University of Maryland at Baltimore County, and the University of Florida. Together, members of the project propose to develop and demonstrate intelligent, dynamic technologies for integrating supply-chain planning, scheduling, and execution and enabling the multi-enterprise integration to evolve in step with changing circumstances. One practical goal was to create the building blocks of a distributed computing environment that accommodate diversity in the processes, practices, and software of supply-chain members. Another was to develop methods, embedded in executing software, for evaluating supply-chain designs and for facilitating collaboratively made changes in those designs. Four research foci were highlighted in this effort. They include: multi-enterprise integrated collaboration support; support for secure multi-enterprise transactions; rule and constraint-based support to knowledge

management and integration; and customer scenario identification and design.

The EECOMS project desired multi-enterprise integration solutions that provided not only greater efficiency across supply chains, but also a degree of synergy among supply chain participants and their business processes. In the following, we highlight three key lessons learned from the EECOMS experience.

3 LESSON ONE: PEOPLE ARE ESSENTIAL PARTICIPANTS IN ENTERPRISE INTEGRATION

One of the pillars to the EECOMS research effort was in a technology we described as Virtual Situation Rooms (VSR) (Tolone, 2000). The original objective of the VSR technologies was to create shared information spaces supported by asynchronous and real-time collaboration technologies to provide command and control-like support (following the military situation room analogy) to facilitate the resolution of integration problems by supply chain participants. Early on in the research process it became clear that providing collaboration support merely for exception resolution was insufficient. In fact, it uncovered a fundamental flaw with the current industry held view that enterprise integration is primarily a problem of automation. To underscore the significance of this problem, we offer several illustrations of common occurrences that become problematic when using even the most current automation-centric EI solutions.

3.1 Narrow view of business processes

In general, business processes, while often described as repeatable, are rarely completely prescriptive. Yet, current EI solutions are designed specifically to support activities that are more prescriptive in nature.

Consequence: "Exceptional" activities, while often handled best as part of "normal" business processes, end up removed from these processes. This leads to business processes that are fragmented between prescriptive and exceptional activities though it is more appropriate and effective to handle these activities together (Hammer, 1996). Moreover, as business processes are further deconstructed so that they are more amenable to automation, they are simultaneously becoming more distributed. Timely and accurate awareness to the state, progress, participants, responsibilities and data relative to these processes, is increasingly essential but more difficult to maintain. As processes become more distributed, the lack of planning for human partici-

pation usually means that human needs for communication and collaboration media are not considered.

3.2 Disconnect between people and business processes

Current EI solutions tend to remove people from or inadequately incorporate people into business processes. (Billings, 1997) Automation increases the speed at which business data can be processed. However, increased data processing speed alone does not reduce the time needed or the effectiveness of the decision-making. The key to achieving increased quality, effectiveness and speed is the timely and appropriate participation of people.

Consequence: Human participation in business processes becomes increasingly difficult because current EI solutions can cause people to be relegated to ineffective functions and increase the dependency of an enterprise on automated decisions. If effective human roles are not properly maintained, a greater frequency of misjudgments is likely. (Tolone, 1998) But maintaining proper roles is extremely difficult, error prone, and time consuming, requiring answers to questions such as "What data are relevant?" "How should they be represented?" and "Who should be involved?" Unfortunately, decision-makers are often provided too much data, as well as data that are insufficient, untimely, improperly formatted, or simply incorrect. This results in people having inaccurate mental models upon which decisions are made. For example, in the aviation industry as automation was added to the cockpit, there were times when "pilots have simply not understood what automation was doing, or why, or what it was going to do next." (Billing, 1997) Similar challenges face enterprise integration, as people cannot be eliminated from decision-making processes.

3.3 Scope Expansion

Current EI solutions increase the scope of business processes while ignoring the inherent complexities introduced by this change in scope. As a result, the role of decision-makers is extended, for example, up and down the manufacturing supply chain or across a wider range of caregivers in healthcare.

Consequences: First, this expansion fosters a lack of understanding of the impact of decisions on both upstream and downstream activities. Prior to the introduction of EI solutions, the effects of activities were far more localized. Second, this confusion increases the difficulty of assigning management responsibility within and across business processes. That is, it is difficult to answer the question "Who is responsible and in control?" Is it the EI solution or a person? How do we answer this question now that the business

processes extend across enterprises? True integration of humans and automation actually requires solutions that eliminate disconnects and seamlessly support the balance of control between automation and human interaction. (Gelernter, 1991) Third, the extension of decision-making scope usually ignores the importance of communication and collaboration to support these newly extended business processes. (Hammer, 1996, Tolone, et al, 1998).

3.4 EECOMS Solutions

Thus, the view that enterprise integration is equivalent to the automation of repeatable business processes is insufficient. Rather, enterprise integration solutions must promote an effective mix of human decision-making and automation. In fact, synergistic solutions require human participation because ultimately it is people that bring synergy to enterprise integration. Automation technologies will never produce benefits greater than the sum of their parts because automation is fundamentally about efficiency and not synergy.

How, then, did this view impact our research? This growing understanding of the human side of enterprise integration affected Virtual Situation Room research and development in four important ways.

First, VSR became an equal participant within the EECOMS integration architecture. Traditionally, collaborative systems, particularly real-time collaboration support, were islands of technology. The VSR research team, however, incorporated the VSR technologies into the integration architecture in such a way that enabled VSR to be an active participant in multi-enterprise transactions.

Second, we began to see collaboration support not as a fixed set of services or facilitates but an evolving, pluggable set based on business process requirements. Consequently, VSR technologies emerged

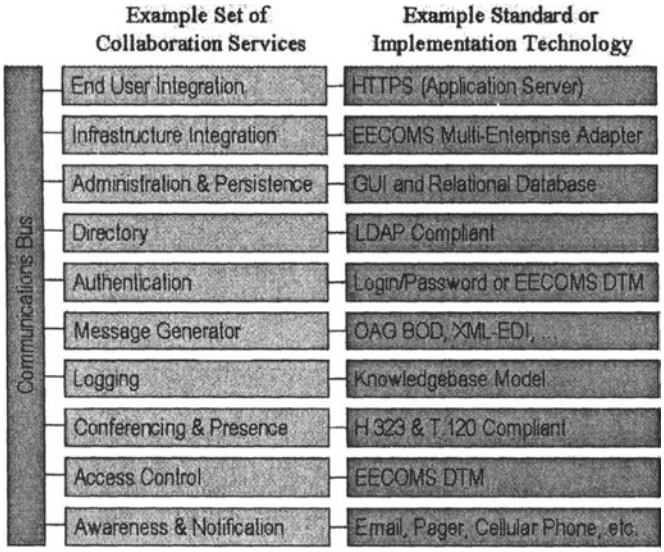

Figure 1: VSR Conceptual Architecture

not as a tightly coupled, monolithic application but rather as a loosely coupled component-based application. Fig. 1 depicts a high-level version of the VSR conceptual architecture and set of collaboration services, as it existed near the conclusion of the project.

Third, collaboration support, and thus VSR, share the same security concerns and problems that face multi-enterprise application integration. Thus, VSR was designed to leverage directly the security results of the EECOMS Project (see the following lesson). Finally, a multi-enterprise collaboration architecture must pervade the integration architecture rather than be a participant within it, i.e. collaboration and integration must be design cooperatively from the ground up so that they may be seamlessly integrated, leveraging common services. Just as security and privacy cannot be add-ons, the same is true for collaboration. While VSR research addressed each of these concerns to some degree, each constitutes a research problem whose magnitude far exceeds the capabilities of a single three-year project; and thus, are a part of a continuing research effort at UNC Charlotte.

To summarize, then, through the EECOMS Project, we learned more deeply that enterprise integration is not solely a problem of automated inter-enterprise transactions (i.e. automatic data synchronization), but truly an enterprise synchronization problem, where enterprises support business processes as the integration of people, applications, practices, and data transactions. This vision is fundamentally different than the automated/data-centric approaches of the past and it provides an appropriate framework for the next generation of EI.

4 LESSON TWO: SECURITY AND PRIVACY ARE INTEGRAL TO ENTERPRISE INTEGRATION

One of EECOMS' principle objectives was to send information across organization boundaries. Over the life of the project, our appreciation for the complexity of this challenge evolved. At the outset, secure integration was primarily a problem of enabling application adapters to communicate securely across enterprise boundaries. While clearly essential to secure integration, this problem is just the first in a series of challenges that must be faced. In fact, the project's security research team was able to attain effective results to this challenge early in the project. Through that effort, though, additional security and privacy issues that are essential to secure integration emerged, resulting in a reformulating of the security research agenda. In the following, we highlight this new agenda and discuss in more detail an open security and privacy issue that emerged near the end of the project.

As the EECOMS Project refined its security agenda, proper authentication and authorization of multi-enterprise transactions emerged as a central issue. Current commercial systems, then and now, do not offer satisfactory solutions to these issues for several important reasons. In today's dynamic work environment with frequent changes in personnel and responsibilities, it is very difficult to manage passwords and access rights within a single organization. It is harder to track users across organization boundaries. Partly due to the challenges of large number of users, most systems do not implement fine levels of access control. An important requirement for integrated multi-enterprise architecture is a model that would allow distributed and scalable management of access rights. Such a model must be easily tied to legal policies where companies decide who and what information should be shared as well as providing an easily traceable audit trail to enforce access policies.

4.1 EECOMS Solutions

During EECOMS we developed a distributed trust management access control model based on digital signatures as well as delegation of access privileges (Chu, Tan, 2000). We believe recent developments in attribute certificates and Privilege Management Infrastructure (PMI) provides the right tools towards establishing such a scalable access control model.

PMI proposes a certificate-based scalable and interoperable authorization solution to enterprise integration (ITU, 2001, Farrel, Housley, 2001). However the roles model in PMI is so primitive that it lacks some advanced components such as role hierarchies and constraints that are core components in role-based access control (RBAC) reference models (Sandhu, et al, 1996). RBAC has been acclaimed and proven to be a simple, flexible, and convenient way of access control management (Sandhu, et al, 1996, Ferraiolo, et al, 1995). Our objective is to investigate how RBAC components can be designed and realized on PMI so that we may enhance authorization services to enterprise integration using a notion of PMI's roles model. In addition, the necessities of security architectures for presiding over the marriage of these two technologies are explored. We also demonstrate the feasibility of the architectures by providing the proof-of-concept prototype implementation.

PMI is a collection of attributes certificates, attribute authorities, repositories, entities involved such as privilege asserters and verifiers, objects, and object methods (ITU, 2001). The attribute certificate binds entities to attributes, which may be the entities' role or group information. PMI introduces its roles model by defining two different types of attribute certificates: *role assignment certificate* and *role specification certificate. Role assignment certificate* has the binding information of an entity and its associated roles,

while *role specification certificate* contains the binding information of the role and its associated privilege policies. In RBAC, roles are defined as job functions or job titles within an organization, users are associated with appropriate roles, and permissions are assigned to roles. It is the roles associated with the users that restrict access to objects, not the ACLs on the object. Thus RBAC makes it simpler and more convenient to manage permissions, reducing the complexity of administrative tasks. It also enables centralized and consistent management of access control policy (Ahn, Sandhu, 2000). RBAC and PMI are complementary, positively producing an alternative authorization solution to enterprise integration.

We developed several system architectures for authorization services based on RBAC and PMI. Push and pull modes in handling attribute certificates introduce four different system architectures. Fig. 2 shows one of these architectures. It consists of three components: *privilege asserter*, *privilege verifier*, and *PMI attribute authority*. *Privilege asserter* is a client application working on behalf of an individual. The individual can request and retrieve *role assignment certificate* from *PMI attribute authority*, or request services (such as access requests to protected resources) using this client application.

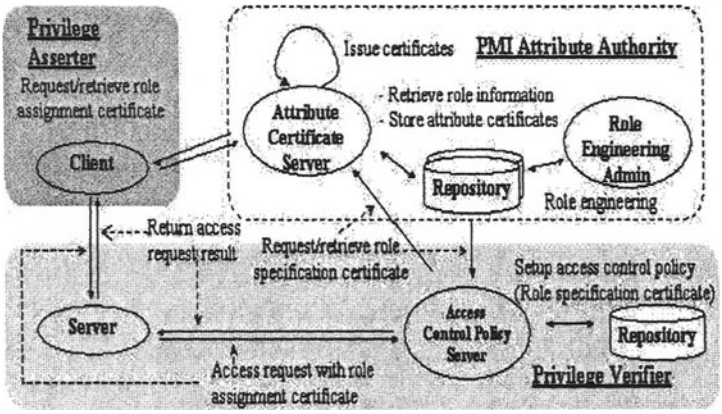

Figure 2: Secure System Architecture (Push mode)

Privilege verifier is composed of server, access control policy server, and repository. Server maintains protected resources or applications. When a client wants to access the server, the server asks the access control policy server whether or not the client has appropriate access privileges. Repository is the data storage for caching the received attribute certificates. As an access control management server, the access control policy server handles access control decisions based on the specified access control policies. Like *privilege verifier, PMI attribute authority* has three components: attribute certificate server, repositories, and role engineering administration. Intuitively, attribute certificate server manages all requests of *role assignment certificate* and *role*

specification certificate issuances. After issuing those certificates, it stores them into a publicly accessible repository. Role engineering administration is an entity performing role-engineering tasks such as role management, user-role assignment, policy specification, and so on.

In summary, PMI is an emerging authorization infrastructure, providing an interoperable and scalable privilege management solution through the use of attribute certificates. RBAC can add simplicity, flexibility, and convenience to PMI through its advanced components such as role-hierarchies and constraints. Privilege management is becoming one of the critical components in designing, developing, and deploying enterprise applications. We believe that our work contributes to the enterprise integration as well as RBAC research communities.

5 LESSON THREE: EFFECTIVE ENTERPRISE INTEGRATION OFTEN REQUIRES A RE-EXAMINATION/DEFINITION OF TRADITIONAL BUSINESS PROCESSES

The EECOMS project planned to demonstrate its multi-enterprise technology by implementing various integrated customer scenarios. One can view these scenarios as expanded use cases integrating various enterprise applications to support business processes. During the project it became obvious that (a) multi-enterprise integration as the "gluing" of existing enterprise-level processes in most cases leads to a less than optimal integration solution, and (b) the combination of the human collaborative technology, automated business rules, and the underlying security technology could provide a novel, synergistic solution to multi-enterprise integration.

5.1 EECOMS Solutions

As a result of this observation, a team led by our customer technology partners identified and designed several customer scenarios. Most notable among this group due to its unique integration of project technologies and design for multi-enterprise integration came to be known as Scenario X. This scenario extended the well-known "available to promise" business process in the following ways. First, it allowed a human team to determine at design time the cost and supply in a series of "what-if" fulfillment to promises. Thus, this multi-enterprise integration scenario runs counter to the trend of gaining efficiency through automation and the elimination of human participation. Rather this scenario was designed with people as central to its effec-

tive and efficient execution. Second, this scenario leveraged input from multi-directional enterprise rules thus enabling the human team the ability to role-play during "what-if" analysis (e.g. participate as: the buyer in a multi-tier supply chain; the collector of critical business rules from third and forth party enterprises; etc.). Third, though not necessarily an extension to the "available to promise" process, demonstration of Scenario X (and others) was completed within an environment that leveraged the requisite security and privacy advances identified and developed through the project. By combining these results iteratively, the multidiscipline product design team functioned as an integral participant within a secure multi-enterprise integration process and understood more efficiently and effectively the availability consequences of their designs, actions and plans.

6 EECOMS PROJECT REFLECTIONS

As we look back on the EECOMS experience we reflect on a very successful and rewarding experience. Through the research and development efforts, a better understand of the research problems, and requisite solutions, were gained. The challenges we faced were not unlike those faced by many large research and development efforts. Yet, our greatest challenges were also our most unique and at the same time our greatest resources. The partnership among industry (including competitors), government, and academia constantly challenged the project while simultaneously providing a rich and diverse background of expertise and experience upon which the project constantly drew.

We confronted early a problem that faces many large research and development projects like EECOMS, specifically those with many commercial partners and universities. This problem is a heightened tendency to create new or abandon all together sound project and business processes. This lapse of project management is done under the guise of reducing overhead, fast tracking, breakthrough thinking, and freedom for research. Yet, this decision can cause extreme trauma to the very people that it is suppose to help. Individual project members often find it very difficult to perceive and react timely to new or changed technical requirements, inter-disciplinary dependences, risk mitigations, or priority scope modifications. When changes occur in project scope and direction, e.g. EECOMS security research effort, good project management practices and good business processes allow a clear direction and a firm team commitment to the change. Abandoning sound processes make the measurement of what is accomplished and what is needed difficult, if not impossible.

In addition to the diversity of our partnership and our adherence to sound project management practices, we also found our decision to drive research and development from a business scenario prospective to be immensely beneficial. Our approach was based on the use case approach advocated by Jacobson (Jacobsen, et al, 1992) and the Unified Software Process (Jacobsen, et al, 1999), although adapted somewhat to focus on multi-enterprise use cases, or what we called customer scenarios. Lesson Three summarizes some of the lessons learned from this approach.

Finally, one of the most beneficial aspects of the EECOMS experience was the taking of research results to an independent technical advisory board and to conference room deployments for review. These regular deployments at partner sites and advisory board reviews provided a valuable source of feedback from both customers and research experts, respectively. These efforts play an invaluable role in enabling partners to commercials research solutions more quickly.

7 SUMMARY

In this paper, we presented three "lessons learned" by the EECOMS Project about the challenges to multi-enterprise integration. These lessons reflect the human side of enterprise integration, the integral role of security and privacy, and the re-examination/definition of traditional business processes that enterprise integration requires.

The EECOMS Project completed its operation in 2001. While the Project Partners' commercialization plans are proprietary and confidential, it can be generally stated that the migration of research results, which began within a year of the Project's inception, is continuing and in specific instances having significant impact on the quality and effectiveness of Partner solutions.

8 REFERENCES

Ahn, G. Sandhu, R. (2000), *Role-based Authorization Constraints Specification*, ACM Transactions on Information and System Security, 3(4).

NIST ATP Project, 97-05-0020, (1998), *EECOMS: Extended Enterprise Consortium for Integrated Collaborative Manufacturing Systems,* CIIMPLEX Consortium. See www.ciimplex.org.

Billings, C. (1997), *Aviation Automation: The Search for a Human-Centered Approach,* Lawrence Erlbaum Associates, Publishers, Mahwah, New Jersey.

CIIMPLEX http://www.ciimplex.org.

Chu, B. Tan, K. (2000), *Distributed Trust Management for Business-to-Business e-Commerce Security,* In *Proceedings of the ACME 2000 International Conference.*

Ferraiolo, D. Cugini, J. and Kuhn, D.R (1995), *Role Based Access Control: Features and Motivations*, In *Annual Computer Security Applications Conference*, IEEE Computer Society Press.

Farrell, S. Housley, R. (2001), *An Internet Attribute Certificate Profile for Authorization,* PKIX Working Group.

Hammer, M. (1996), *Beyond Reengineering*. Harper Business, New York.

ITU-T Recommendation X.509, (2001), *Information Technology: Open Systems Interconnection - The Directory: Public-Key And Attribute Certificate Frameworks*, ISO/IEC 9594-8.

Gelernter, D. H. (1991), *Mirror Worlds or: THE DAY SOFTWARE PUTS THE UNIVERSE IN A SHOEBOX...HOW IT WILL HAPPEN AND WHAT IT WILL MEAN.* Oxford Univ. Press.

Jacobson, I. Booch, G. Rumbaugh, J. (1999), *The Unified Software Development Process*. Addison Wesley.

Jacobson, I. Christerson, M. Jonsson, P. Övergaard, G. (1992), *Object-Oriented Software Engineering: a Use Case Driven Approach*. Addison-Wesley.

Sandhu, R. Coyne, E.J. Feinstein, H.L. Youman, C.E. (1996), *Role Based Access Control Models*, IEEE Computer 29 (2).

Tolone, W. J. Chu, B. Long, J. Wilhelm, R. G. Finin, T. Peng, Y. Boughannam, A. (1998), *Supporting Human Interactions within Integrated Manufacturing Systems,* International Journal of Agile Manufacturing, Vol. 1(2).

Tolone, W. J. (2000), *Virtual Situation Rooms: Connecting People Across Enterprises for Supply Chain Agility*. Journal of Computer-Aided Design, Elsevier Science Ltd. Vol. 32(2).